CLAIMS

What is claimed is:

1. A group management system comprising:

   a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"); and

   a plurality of master nodes, each of the master nodes controlling membership in the VPN for an associated non-empty subset of the member nodes.

2. The system of claim 1wherein a membership change in at least one of the subsets can be performed without notifying all of the master nodes not associated with the changed subset.

3. The system of claim 1 wherein at least two of the subsets do not share any member nodes in common.

4. The system of claim 1 wherein at least two of the subsets share at least one member node in common.

5. The system of claim 4 wherein a communication involving said common member node can be transmitted along multiple paths.

6. The system of claim 5, further comprising an intrusion detection mechanism that receives said multiple-path communication as input.

7. The system of claim 1 wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes.

8. The system of claim 7, wherein each of the member nodes is associated with at least one of the master nodes as a back-up master.

9. The system of claim 1 wherein the plurality of interconnected nodes are communicatively coupled as part of a peer-to-peer network.

10. The system of claim 1 wherein the plurality of master nodes are part of an edge-based content delivery network.

11. The system of claim 1 wherein the member nodes are allocated to the subsets at least partly based upon one or more criteria of connectivity between each of the member nodes and the corresponding master nodes.

12. The system of claim 11 wherein the connectivity criteria are selected from a group of criteria comprising geographical distance, topological distance, bandwidth, latency, jitter, financial cost, and political boundaries.

13. The system of claim 1 wherein at least one of the master nodes further controls membership in another virtual overlay group different from the VPN.

14. The system of claim 1wherein a communication from a first one of the subsets of the member nodes uses a first encryption key, and a communication from a second one of the subsets uses a second encryption key that is different from the first encryption key.

15. The system of claim 14, wherein one or more of the master nodes are operable to translate between the encryption keys.

16. The system of claim 1wherein a communication from a first one of the subsets of the member nodes and a communication from a second one of the subsets of the member nodes both use the same encryption key.

17. The system of claim 1 wherein at least one of the master nodes are operable to remotely install software communication mechanisms for a new member node of the VPN without the necessity of installing augmented hardware for the new member node.